AsyncOS 15.0.1 for Cisco Secure Email Cloud Gateway リリースノート（メンテナンス導入）

発行日：2023 年 11 月 30 日

改訂日：2024 年 2 月 13 日

目次

Cisco Systems, Inc.
www.cisco.com

今回のリリースでの変更点

AsyncOS 15.0.1 の新機能

このリリースで追加された新機能はありません。このリリースの既知および修正済みの問題のリストについては、既知および修正済みの問題（19 ページ）を参照してください。

AsyncOS 15.0 の新機能

機能	説明
送信者レベルまたは受信者レベルでの発信メッセージに対する TLS の適用	既存の送信先コントロール設定を使用して、ドメインごとに TLS モード（TLS 必須、TLS 推奨など）を上書きできます。 送信者、受信者などの追加の条件に基づいて発信メッセージに TLS を適用する必要がある場合は、`X-ESA-CF-TLS-Mandatory` ヘッダーを使用できるようになりました。 [コンテンツフィルタ–ヘッダーの追加/編集（Content Filter – Add/Edit Header）] アクションを設定して、コンテンツフィルタ条件に基づいて [ヘッダー名:（Header Name:）] フィールドに `X-ESA-CF-TLS-Mandatory` ヘッダーを追加し、コンテンツフィルタを発信メールポリシーにアタッチできます。
グレイメール登録解除バナーのカスタマイズ	組織の要件に基づいて、グレイメール登録解除バナーの次の設定をカスタマイズできます。 • バナーの位置 • バナーの色 • バナーメッセージのテキストの色 • バナーメッセージの内容 バナーメッセージは、英語（米国）、イタリア語、中国語、ポルトガル語、スペイン語、ドイツ語、フランス語、ロシア語、日本語、韓国語、中国語（台湾）をサポートしています。 **（注）** このリリースでは、この機能に対する CLI サポートはありません。 詳細については、ユーザーガイドの「Managing Spam and Graymail」の章にある「Customizing Graymail Unsubscribe Banner based on Organizational Requirements」のセクションを参照してください。

脅威検出効果の向上	以下により、電子メールゲートウェイのセキュリティが向上しました。 • HTML 解析と悪意のあるスクリプト検出の改善。 • URL 解析とリダイレクト検出の改善。 この機能を使用するには、次の設定手順を実行します。 1. 次のいずれかの方法で、電子メールゲートウェイで**グレイメール** サービス エンジンをグローバルに有効化します。 **Web インターフェイス**:[セキュリティサービス(Security Services)] > [IMS およびグレイメール(IMS and Graymail)] ページに移動し、[グレイメールのグローバル設定(Graymail Global Settings)] の下にある [グレイメール検出(Graymail Detection)] チェックボックスをオンにします。 **CLI**:`graymail` > `setup` サブコマンドを使用し、次のステートメントに対して **yes** と入力します:「`Would you like to use Graymail Detection? [Y]>`」 2. 次のように、必要な受信メールポリシーの**スパム対策サービス** エンジンを有効にします。 a. Web インターフェイスで、[メールポリシー(Mail Policies)] > [受信メールポリシー(Incoming Mail Policies)] ページに移動します。 b. [ポリシー(Policies)] フィールドの [スパム対策(Anti-Spam)] の下にある [無効(Disabled)] リンクをクリックします。 c. [IronPort スパム対策サービスを使用(Use IronPort Anti-Spam service)] または [IronPort インテリジェントマルチスキャンを使用(Use IronPort Intelligent Multi-Scan)] オプションボタンのいずれか該当するほうを選択して、メールポリシーのスパム対策スキャンを有効にします。 d. 陽性と判定されたスパムメッセージに適用する必要なアクション(「配信(deliver)」、「ドロップ(drop)」、「スパムの隔離(spam quarantine)」、または「バウンス(bounce)」のいずれか)を選択します。 e. [オプション]:その他必要なスパム対策の設定を行います。 f. [送信(Submit)] をクリックし、変更をコミットします。 脅威検出の改善によりメッセージが「スパム」に分類されたことを示す新しい判定である **ThreatScanner スパム陽性**が、メッセージトラッキングとメールログに追加されました。**ThreatScanner スパム陽性**判定に対して推奨されるスパム対策ポリシーアクションは、[隔離(Quarantine)] です。 スパム理由データを含む**グレイメール**ログは、**情報**ログレベルで利用できます。

ファイル レピュテーション サービスの強化	AsyncOS 15.x リリース以降、電子メールゲートウェイは新しいバージョンの AMP エンジンを使用しています。この新しい AMP エンジンは、TCP の代わりに HTTPS（ポート 443）を使用して、電子メールゲートウェイと Cisco Secure Endpoint Cloud 間の安全な通信を保証します。 **（注）** [Cisco Secure Endpoint プライベート クラウド ユーザーのみ]：このリリースにアップグレードする前に、新しいファイル レピュテーション サービスのアクティブ化の前提条件をすべて満たしていることを確認してください。詳細については、このドキュメントの「アップグレード前の注意事項」の項の「ファイル レピュテーション サービスのアクティブ化の前提条件 - Cisco Secure Endpoint プライベート クラウド」サブセクションを参照してください。 **（注）** [Cisco Secure Endpoint プライベート クラウド ユーザーのみ]：アップグレード中にファイル レピュテーション サービスのアクティブ化に関する手順をスキップした場合は、アップグレード後のファイル レピュテーション サービスのアクティブ化方法について、このドキュメントの「アップグレード後の注意事項」の項にある「Vault の問題を解決するための Vault Recovery スクリプトの実行」サブセクションを参照してください。 詳細については、ユーザーガイドの「File Reputation Filtering and File Analysis」の章を参照してください。
電子メールゲートウェイからのログファイルの削除	電子メールゲートウェイの /data/pub/directories パスに保存されているログファイルを削除できるようになりました。 CLI の `logconfig` > `deletelogfile` サブコマンドを使用してログファイルを削除できます。 **（注）** 電子メールゲートウェイがクラスタ内にある場合、`deletelogfile` サブコマンドはマシンレベルのオプションです。 詳細については、このリリースに関連する CLI リファレンスガイドの「Example- Deleting Log Files」の項を参照してください。
FIPS 認定	Cisco Secure Email Gateway は FIPS 認定され、FIPS 140-2 認定の暗号化モジュール、Cisco Common Crypto Module を統合しました（FIPS 140-2 認定 #4036）。 詳細については、このリリースに関連するユーザーガイドの「FIPS Management」の章を参照してください。
システムアップグレード中の脆弱なアルゴリズムの削除に関する新しい注記	[FIPS および非 FIPS モードに適用]：AsyncOS 15.0 以降へのシステムアップグレード時、暗号、キー、KEX、および MAC（設定されている場合）のすべての脆弱なアルゴリズムがアップグレードプロセス後にシステムによって削除されることを通知する新しい注意文が追加されました。

AsyncOS API を使用した設定情報の取得	設定 API を使用して、電子メールゲートウェイでさまざまな操作（作成、取得、更新、削除など）を実行できます。設定の各種 API カテゴリは次のとおりです。 • 認証 API • URL リスト API • ディクショナリ API • ホストアクセステーブル（HAT）API **（注）** 構成 API の場合、管理者およびクラウド管理者のユーザーロールのみがサポートされています。 **（注）** 構成 API の場合： - クラスタモードでいずれかの API を変更すると、その変更はクラスタ内の他のすべてのマシンに適用されます。 - グループモードでいずれかの API を変更すると、その変更はグループ内の他のすべてのマシンに適用されます。 - マシンモードでいずれかの API を変更すると、その変更は指定されたマシンにのみ適用されます。 詳細については、『AsyncOS 15.0 API for Cisco Secure Email Gateway - Getting Started Guide』の「Configuration APIs」セクションを参照してください。
電子メールトラッキングデータ用の古い Splunk データベースの削除	Cisco Secure Email Gateway 15.0 以降にアップグレードし、電子メールトラッキングデータが Splunk データベースに含まれている場合、アップグレードを続行すると、システムによって Splunk データベースが削除されます。 **（注）** Splunk データベースのデバッグ情報を収集するために使用される `debug` サブメニューは、CLI の `Diagnostic > Tracking` サブコマンドから削除されました。
Cisco Secure Email Gateway 仮想アプライアンスモデルの新しい RAM 値	AsyncOS 15.0 リリース以降では、KVM または VMWare ESXi を介して展開された次の Cisco Secure Email Gateway 仮想アプライアンスモデルに新しい RAM 値があります。 • C100V • C300V • C600V 各仮想アプライアンスモデルに該当する新しい RAM 値の詳細については、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。このドキュメントは、https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html から入手できます。

事前定義された DLP ポリシーの新しい分類子	次の事前定義された DLP ポリシーの新しい分類子が、Web インターフェイスの [メールポリシー（Mail Policies）] > [DLP ポリシーマネージャ（DLP Policy Manager）] > [DLP ポリシーの追加（Add DLP Policy）] > [カスタムポリシー（Custom Policy）] > [追加（Add）] > [ポリシー一致の詳細（Policy Matching Details）] ページに追加されます。 • 銀行口座番号（オーストリア IBAN） • 銀行口座番号（ベルギー IBAN） • 銀行口座番号（ブルガリア IBAN） • 銀行口座番号（クロアチア IBAN） • 銀行口座番号（キプロス IBAN） • 銀行口座番号（チェコ共和国 IBAN） • 銀行口座番号（デンマーク IBAN） • 銀行口座番号（エストニア IBAN） • 銀行口座番号（フィンランド IBAN） • 銀行口座番号（ギリシャ IBAN） • 銀行口座番号（ハンガリー IBAN） • 銀行口座番号（アイルランド IBAN） • 銀行口座番号（ラトビア IBAN） • 銀行口座番号（リトアニア IBAN） • 銀行口座番号（ルクセンブルク IBAN） • 銀行口座番号（マルタ IBAN） • 銀行口座番号（ポーランド IBAN） • 銀行口座番号（ポルトガル IBAN） • 銀行口座番号（ルーマニア IBAN） • 銀行口座番号（スロバキア IBAN） • 銀行口座番号（スロベニア IBAN） • 銀行口座番号（スペイン IBAN） • カンボジア国民 ID • キプロス国民 ID • フィンランド国民 ID • マルタ国民 ID • ミャンマー国民 ID • ポルトガル国民 ID • ベトナム国民 ID

SSL 通信の ECDSA 証明書のサポート	楕円曲線デジタル署名アルゴリズム(ECDSA)証明書を使用して、キー交換と ECDSA 認証に楕円曲線 Diffie-Hellman Ephemeral (ECDHE)アルゴリズムを組み合わせ、次の SSL サービスを設定できるようになりました。 • GUI HTTPS • インバウンド SMTP

動作における変更

AsyncOS 15.0.1 の動作の変更

バウンスプロファイルの削除:新しいステータスメッセージ	このリリース以降、バウンスプロファイルを削除すると、削除確認メッセージが表示されるまで、[バウンスプロファイル(Bounce Profile)] ページの左上隅に「**処理中**」ステータスメッセージが表示されます。
TG 分析のためのアーカイブファイルのアップロード	このリリースより前は、電子メールゲートウェイで抽出に失敗したアーカイブファイルは、分析のために Threat Grid(TG)にアップロードされていました。 このリリース以降、電子メールゲートウェイで抽出に失敗したアーカイブファイルは、分析のために TG にアップロードされません。

AsyncOS 15.0 での動作の変更

送信者ドメイン レピュテーション フィルタリング:ドメイン例外リストの変更	[このリリースの前]:[Envelope From:のドメインに基づいてドメイン例外リストを照合(Match Domain Exception List based on Domain in Envelope From:)] オプションを無効にすると、メッセージの「Envelope From:」、「From:」、および「Reply-To:」ヘッダーのドメインが同じであり、ドメイン例外リストにある場合にのみ、メッセージがドメイン例外リストと照合されます。 [このリリース以降]:[Envelope From:のドメインに基づいてドメイン例外リストを照合(Match Domain Exception List based on Domain in Envelope From:)] オプションを無効にすると、メッセージの「Envelope From:」、「From:」、および「Reply-To:」ヘッダーのドメインが異なり、「HELO:」、「RDNS:」、「Envelope From:」、「From:」、および「Reply-To:」のいずれかのドメインがドメイン例外リストにある場合でも、メッセージがドメイン例外リストと照合されます。

RFC 違反のため、メッセージをスキャン不可（Unscannable）として分類する新しい条件	[このリリースの前]: メッセージの MIME 部分に複数の「Content-Transfer-Encoding」ヘッダーが含まれている場合、コンテンツスキャナは RFC 違反によりメッセージを「スキャン不可（Unscannable）」として分類しませんでした。 [このリリース以降]: MIME 部分に複数の「Content-Transfer-Encoding」ヘッダーが含まれている場合、コンテンツスキャナは RFC 違反のため、メッセージを「スキャン不可（Unscannable）」として分類します。「セキュリティサービス（Security Services）> スキャン動作（Scan Behavior）> RFC 違反が原因でメッセージをスキャンできない場合のアクション（Action when a message is unscannable due to RFC violations）」で設定されたアクションがメッセージに適用されます。
Syslog メッセージの変更	[このリリースの前]: Syslog メッセージには、電子メールゲートウェイの設定済み IP アドレスが表示されていました。 [このリリース以降]: Syslog メッセージに IP アドレスは表示されませんが、電子メールゲートウェイの設定された FQDN またはホスト名が表示されるようになりました。
[アップグレードのシナリオ]: SSH サーバーとクライアントの設定の変更	電子メールゲートウェイを下位の AsyncOS バージョンから AsyncOS 15.0 バージョン以降にアップグレードする場合は、次の SSH サーバーとクライアントの設定の変更が適用されます。 [非 FIPS モードのみ]: 電子メールゲートウェイが FIPS モードでない場合に適用される、SSH サーバーおよびクライアントの設定の変更は次のとおりです。 [SSH サーバーの設定の変更]: • 次の暗号アルゴリズム、MAC メソッド、KEX アルゴリズム、およびホストキーアルゴリズムは、デフォルトで電子メールゲートウェイから削除されます。 – **暗号アルゴリズム**: `3des-cbc` および `rijndael-cbc@lysator.liu.se` – **MAC メソッド**: `hmac-md5`、`umac-64@openssh.com`、`hmac-ripemd160`、`hmac-ripemd160@openssh.com`、`hmac-sha1-96`、および `hmac-md5-96` – **KEX アルゴリズム**: `diffie-hellman-group-exchange-sha256` および `diffie-hellman-group-exchange-sha1` – **ホストキーアルゴリズム**: `rsa1` • [最小サーバーキー（Minimum Server Key）] オプションは、デフォルトで電子メールゲートウェイの CLI から削除されます。 • ホストキーアルゴリズム - `rsa-sha2-256` は、デフォルトで電子メールゲートウェイに追加されます。 [SSH クライアント設定の変更]: • 暗号アルゴリズム - `arcfour256` および `arcfour128` は、デフォルトで電子メールゲートウェイから削除されます。 • ホストキーアルゴリズム - `rsa-sha2-256` は、デフォルトで電子メールゲートウェイに追加されます。

[アップグレードのシナリオ]:SSH サーバーとクライアントの設定の変更（続き）	[FIPS モードのみ]:電子メールゲートウェイが FIPS モードである場合に適用される、SSH サーバーおよびクライアントの設定の変更は次のとおりです。 [SSH サーバーの設定の変更]: • 次の暗号アルゴリズム、KEX アルゴリズム、およびホストキーアルゴリズムは FIPS 非準拠であり、電子メールゲートウェイから削除されます。 – **暗号アルゴリズム**:`3des-cbc` – **KEX アルゴリズム**:`diffie-hellman-group-exchange-sha256` および `diffie-hellman-group-exchange-sha1` – **ホストキーアルゴリズム**:`ssh-rsa` • [最小サーバーキーサイズ（Minimum Server Key Size）] オプションは、FIPS 非準拠であるため、電子メールゲートウェイの CLI から削除されます。 • ホストキーアルゴリズム - `rsa-sha2-256` は、デフォルトで電子メールゲートウェイに追加されます。 • ホスト キー アルゴリズム - `ssh-dss` は、デフォルトで電子メール ゲートウェイから削除されます（CLI で `logconfig` > `hostkeyconfig` サブコマンドを使用して設定されている場合）。 [SSH クライアント設定の変更]: • 暗号アルゴリズム - `3des-cbc` は FIPS 非準拠であるため、電子メールゲートウェイから削除されます。 • ホストキーアルゴリズム - `rsa-sha2-256` は、デフォルトで電子メールゲートウェイに追加されます。

[新規インストールのシナリオ]:SSH サーバの設定変更	次の SSH サーバー設定の変更は、Cisco Secure Email Gateway 用の AsyncOS 15.0 を初めてインストールする場合にのみ適用されます。 [非 FIPS モードのみ]:電子メールゲートウェイでは、次の暗号アルゴリズム、MAC メソッド、KEX アルゴリズム、およびホストキーアルゴリズムがサポートされています。 • **暗号アルゴリズム**:aes128-ctr、aes192-ctr、aes256-ctr、aes128-cbc、aes192-cbc、および aes256-cbc • **MAC メソッド**:hmac-sha1 • **KEX アルゴリズム**:diffie-hellman-group14-sha1、ecdh-sha2-nistp256、ecdh- sha2-nistp384、および ecdh-sha2-nistp521 • **ホストキーアルゴリズム**:rsa-sha2-256、ssh-rsa、および ssh-dss(デフォルトでは無効) **(注)** CLI で shconfig > sshd > setup サブコマンドを使用して、「ssh-dss」暗号アルゴリズムを手動で有効にする必要があります。 --- [FIPS モードのみ]:FIPS モードを有効にするには、まず CLI で sshconfig > sshd > setup サブコマンドを使用して、FIPS 非準拠の次の暗号アルゴリズムおよびホストキーアルゴリズムを無効にします。 • **暗号アルゴリズム**:aes192-ctr • **ホストキーアルゴリズム**:ssh-rsa **(注)** ホストキーアルゴリズム - rsa-sha2-256 が新しく追加され、デフォルトで電子メールゲートウェイで有効になっています。
SPF 電子メール検証の変更	[このリリースの前]:電子メールゲートウェイは、RFC 4408(セクション 4.4)標準に従って、SPF および TXT レコードに基づいて Sender Policy Framework(SPF)電子メール検証プロセスを実行します。 [このリリース以降]:電子メールゲートウェイは、新しい RFC 7208(セクション 4.4)標準に従って、TXT レコードのみに基づいて SPF 電子メール検証プロセスを実行します。
統合イベントログの CEF フィールド名の変更	このリリース以降、統合イベントログの次の Common Event Format(CEF)フィールド名が変更されました。 • 「endTime」から「end」 • 「startTime」から「start」 • 「sourceAddress」から「src」 • 「sourceHostName」から「shost」

ファイル分析のための HTML および Octet-stream ファイルのアップロードにおける変更	[このリリースの前]:ファイル分析用のファイル拡張子が選択されている場合、電子メールゲートウェイは、HTML および Octet-stream ファイル(MIME タイプ:application/octet-stream および text/html)のみをファイル分析サーバーにアップロードできました。 [このリリース以降]:電子メールゲートウェイは、ファイル分析用のファイル拡張子が選択されていない場合でも、ファイル分析のために HTML および Octet-stream ファイルをファイル分析サーバーにアップロードできるようになりました。 (注) ファイル分析サーバーにアップロードされるファイルの数が増えると、電子メールゲートウェイがすぐにファイル分析サーバーのファイルアップロード制限に達する可能性があります。
ファイル分析のためのアーカイブファイルのアップロードにおける変更	[このリリースの前]:AMP エンジンがメッセージからアーカイブファイル(パスワードで保護されアーカイブされた添付ファイルを含む)の抽出に失敗すると、添付ファイルはファイル分析サーバーにアップロードされませんでした。 [このリリース以降]:AMP エンジンがメッセージからアーカイブファイル(パスワードで保護されアーカイブされた添付ファイルを含む)の抽出に失敗した場合に、添付ファイルはファイル分析のためにファイル分析サーバーにアップロードされるようになりました。 (注) ファイル分析サーバーにアップロードされるファイルの数が増えると、電子メールゲートウェイがすぐにファイル分析サーバーのファイルアップロード制限に達する可能性があります。
メッセージスキャンのデフォルトしきい値の変更	[このリリースの前]:インテリジェント マルチスキャン(IMS)およびグレイメールエンジンがメッセージをスキャンしないデフォルトのしきい値は、1 M に設定されていました。 [このリリース以降]:インテリジェント マルチスキャン(IMS)およびグレイメールエンジンがメッセージをスキャンしないデフォルトのしきい値は、2 M に設定されます。
ECDSA および EDDSA 証明書のインポートのサポート	このリリース以降、ECDSA および EDDSA アルゴリズムを使用した x509 証明書のサポートが導入されました。
暗号設定の変更	非準拠/脆弱な TLS 暗号スイートは、インバウンド SMTP、アウトバウンド SMTP、GUI、LDAP、およびアップデータでデフォルトで無効になりました。 `ssh-dss` などの非準拠 CSDL キー SSH アルゴリズムは、デフォルトで SSH サーバーで無効になりましたが、設定することはできます。
自己署名証明書の作成時に署名アルゴリズムを選択するためのサポート	このリリース以降、CLI と GUI の両方で自己署名/自己署名 SMIME 証明書を生成する際に、署名アルゴリズム(sha256withRSAEncryption、sha384withRSAEncryption、または sha512withRSAEncryption)を選択できます。

x509 証明書の署名アルゴリズムの変更	TLS サービス(インバウンド SMTP、スマート ライセンス トランスポート URL サーバー、登録クライアント、SSE サーバー、Talos クライアント、Syslog サーバー、ECS クライアント、および Cisco Security Awareness クラウドサーバー)のピア証明書に次の署名アルゴリズムはサポートされません。 「sha1withrsaencryption」、「sha224withrsaencryption」、「dsawithsha1」、「ecdsa-with-sha1」、「ecsda-with-sha224」、「md2withrsaencryption」、「md4withrsaencryption」、「md5withrsaencryption」、「ripemd128withrsaencryption」、「ripemd160withrsaencryption」、「ripemd256withrsaencryption」、「ripemd128withrsa」、「ripemd160withrsa」、「ripemd256withrsa」 TLS サービス(インバウンド SMTP、スマート ライセンス トランスポート URL サーバー、登録クライアント、SSE サーバー、Talos クライアント、Syslog サーバー、ECS、および Cisco Security Awareness クラウドサーバー)の ECDSA 署名アルゴリズムを使用したピア証明書の次の曲線はサポートされません。 「secp224r1」、「secp192r1」、「brainpoolP160r1」、「brainpoolP192r1」、「secp160r1」、「secp160r2」、「prime192v1」、「secp192k1」、「secp224k1」、「secp256k1」、「sect163k1」、「sect163r2」、「sect193r1」、「sect193r2」、「sect233k1」、「sect233r1」、「sect239k1」、「sect283k1」、「sect283r1」、「sect409k1」、「sect409r1」、「sect571k1」、「sect571r1」
リモートアクセスアカウントの有効期限	このリリース以降、techsupport > sshaccess コマンドを使用して作成されたリモートアクセスアカウントは、7 日間アクティブのままになります。その後は、リモートアクセスを再度有効にする必要があります。 リモートアクセス用のランダムシード文字列を入力するオプションは、Web インターフェイスおよび CLI で削除されました。

アップグレードの方法

リリース 15.0.1-030 - MD(メンテナンス導入)へのアップグレード

次のバージョンから、リリース 15.0.1-030 にアップグレードすることができます。

- 14.2.1-020
- 14.2.2-004
- 14.2.3-027
- 14.2.3-031
- 14.3.0-032
- 15.0.0-097
- 15.0.0-104

リリース 15.0.0-104 へのアップグレード（一般導入）

次のバージョンからリリース 15.0.0-104 にアップグレードできます。

- 13.0.5-007
- 13.5.4-038
- 14.0.0-698
- 14.0.1-033
- 14.0.2-020
- 14.2.0-616
- 14.2.0-620
- 14.2.1-015
- 14.2.1-020
- 14.2.2-004
- 14.3.0-023
- 14.3.0-032
- 15.0.0-097

リリース 15.0.0-097 へのアップグレード（限定導入）

次のバージョンからリリース 15.0.0-097 にアップグレードできます。

- 13.0.5-007
- 13.5.4-038
- 14.0.0-698
- 14.0.1-033
- 14.0.2-020
- 14.2.0-616
- 14.2.0-620
- 14.2.1-015
- 14.2.1-020
- 14.2.2-004
- 14.3.0-023
- 14.3.0-032
- 15.0.0-012
- 15.0.0-048
- 15.0.0-068
- 15.0.0-085

リリース 15.0.0-068 へのアップグレード（限定導入）

次のバージョンからリリース 15.0.0-068 にアップグレードできます。

- 13.0.5-007
- 13.5.4-038
- 14.0.0-698
- 14.0.1-033
- 14.0.2-020
- 14.2.0-616
- 14.2.0-620
- 14.2.1-015
- 14.2.1-020
- 14.2.2-004
- 14.3.0-023
- 14.3.0-032
- 15.0.0-012
- 15.0.0-048

このリリースでサポートされる VM

このリリースでは、次の VM がサポートされています。

- C100V
- C300V
- C600V

アップグレード前の注意事項

アップグレードする前に、次の事項を確認してください。

- AsynOS 15.0.0-xxx から AsynOS 15.0.0-104 GD への電子メールゲートウェイのアップグレード（15 ページ）
- 暗号化通知テンプレートの削除（15 ページ）
- ファイル レピュテーション サービスのアクティブ化の前提条件 - Cisco Secure Endpoint プライベートクラウド（15 ページ）

AsynOS 15.0.0-xxx から AsynOS 15.0.0-104 GD への電子メールゲートウェイのアップグレード

電子メールゲートウェイを AsynOS 15.0.0-xxx から AsynOS 15.0.0-104 GD リリースにアップグレードするとき、「Vault エラー（Vault error）」を示すアラートを受信した場合は、Cisco TAC にお問い合わせください。

これは既知の問題です。不具合 ID：CSCwh15269。

暗号化通知テンプレートの削除

電子メールゲートウェイを AsyncOS 15.0.x にアップグレードすると、アップグレード中に「サポートされていない形式」が含まれていることが検出された既存の暗号化通知テンプレート（HTML またはテキスト形式）は自動的に削除されます。

ファイルレピュテーション サービスのアクティブ化の前提条件 - Cisco Secure Endpoint プライベートクラウド

このリリースにアップグレードする前に、ファイル レピュテーション サービスのアクティブ化に関する次の前提条件を満たしていることを確認してください。

- Cisco Secure Endpoint プライベートクラウドを 3.8.1 以上のバージョンにアップグレードした
- アップグレードプロセス中にプロンプトが表示されたとき、Cisco Secure Endpoint の「コンソールのホスト名」と「アクティベーションコード」の詳細を入力した。

アップグレード後の注意事項

Vault の問題を解決するための Vault Recovery スクリプトの実行

（ハードウェア、オンプレミス、CES、AWS、KVM、Azure、または Hyper-V の）電子メールゲートウェイで Vault 関連の問題が発生した場合、暗号化が**無効**になっているときは、その問題を解決するために Vault Recovery スクリプトを実行する必要があります。Vault Recovery スクリプトを実行するには、次の手順を使用してください。

1. 次のログイン情報を使用して、直接 SSH 接続を介して電子メールゲートウェイにログインします。

   ユーザー名：**enablediag**

   パスワード：**管理者ユーザーのパスワード**

2. `recovervault` コマンドを実行します。
3. プロンプトが表示されたら、次の一連のサブコマンドを入力します。
   a. `yes`
   b. `encryption disable [2]`
   c. `reboot`

   電子メールゲートウェイが回復し、Vault が再初期化されます。

   これで、問題なくシステムに接続でき、すべてのシステム設定が保持されます。

(ハードウェア、オンプレミス、CES、AWS、KVM、Azure、または Hyper-V の)電子メールゲートウェイで Vault 関連の問題が発生した場合、暗号化が**有効**になっているときは、Cisco TAC に連絡してその問題を解決してください。

(注) このシナリオでは、次の暗号化された変数がデフォルトの工場出荷時の値にリセットされます。

- 証明書の秘密キー
- RADIUS パスワード
- LDAP バインドのパスワード
- ローカル ユーザのパスワードのハッシュ
- SNMP パスワード
- DK/DKIM 署名キー
- 発信 SMTP 認証パスワード
- PostX 暗号化キー
- PostX 暗号化プロキシ パスワード
- FTP プッシュ ログ サブスクリプションのパスワード
- IPMI LAN パスワード
- アップデータ サーバの URL
- 認証 API のクライアントログイン情報
- Cisco Advanced Malware Protection プロキシパスワード
- SAML 証明書のパスフレーズ

以前の設定を復元する場合は、以前に保存した設定ファイルをロードする必要があります。

(注) 認証 API のクライアントログイン情報は設定ファイルに保存されないため、API を呼び出して新しいクライアントログイン情報を作成する必要があります。

ログ(enablediag ユーザーの場合):

```
Available Commands:
help -- View this text.
quit -- Log out.
service -- Enable or disable access to the service system.
network -- Perform emergency configuration of the diagnostic network interface.
clearnet -- Resets configuration of the diagnostic network interface.
```

```
ssh -- Configure emergency SSH daemon on the diagnostic network interface.
clearssh -- Stop emergency SSH daemon on the diagnostic network interface.
tunnel -- Start up tech support tunnel to IronPort.
print -- Print status of the diagnostic network interface.
recovervault -- Recover vault, it will only restore the encrypted variables to factory
values, will not touch anything related to configurations if encryption is disabled .
resetappliance -- Reset appliance reverts the appliance to chosen build with factory
default settings with default IP. No network configuration would be preserved.
reboot -- Reboot the appliance.

S/N 42189A47B0D50A645948-CEC55115B364
Service Access currently ENABLED (0 current service logins)
esa1.hc303-10.smtpi.com> recovervault

Are you sure you want to recover vault?  [N]> y
Encryption is enabled [1]>
Encryption is not enabled [2]>
```

Cisco Secure Endpoint プライベートクラウドのファイル レピュテーション サービスのアクティブ化

ファイル レピュテーション サービスをアクティブにするには、システムセットアップに基づいて次のいずれかの手順に従います。

- [クラスタモード]:新しいファイル レピュテーション サービスがすでに設定されている電子メールゲートウェイに接続します。
- [スタンドアロンモード]:次の手順を実行します。

  1. Web インターフェイスで、[セキュリティサービス(Security Services)] > [ファイルレピュテーションと分析(File Reputation and Analysis)] ページに移動します。

  2. [グローバル設定を編集(Edit Global Settings)] ボタンをクリックします。

  3. [ファイルレピュテーションの詳細設定(Advanced Settings for File Reputation)] パネルをクリックします。

  4. [ファイルレピュテーションサーバー(File Reputation Server)] ドロップダウンリストから [プライベートレピュテーションクラウド(Private reputation cloud)] オプションを選択します。

  5. 所定のフィールドにコンソールのホスト名とアクティベーションコードを入力します。

  6. [送信(Submit)] をクリックし、変更をコミットします。

DLP サービスステータスチェック

このリリースにアップグレードした後、DLP サービスで問題が発生する可能性があります。

ソリューション:CLI で `diagnostic` > `services` > `DLP` > `status` サブコマンドを使用して、電子メールゲートウェイの DLP サービスのステータスを確認します。DLP サービスが実行されていない場合は、既知の問題リストにある CSCvy08110 の不具合の「回避策」セクションを参照してください。既知の問題を表示する方法の詳細については、既知および修正済みの問題のリスト（19 ページ）を参照してください。

電子メールゲートウェイでのパスワードで保護された添付ファイルのスキャン

パスワード保護された添付ファイルをスキャンするように電子メールゲートウェイのコンテンツスキャナを設定する場合、電子メールトラフィックにパスワード保護された添付ファイルが高い割合で含まれていると、パフォーマンスに影響を与える可能性があります。

インテリジェント マルチスキャンおよびグレイメールのグローバル設定の変更

AsyncOS 15.0 にアップグレードした後のインテリジェント マルチスキャン（IMS）およびグレイメールのグローバル設定の変更点は次のとおりです。

- IMS およびグレイメールのグローバル設定が異なるクラスタレベルで構成されている場合、電子メールゲートウェイはグローバル設定を最も低い設定レベルにコピーします。たとえば、クラスタレベルで IMS を設定し、マシンレベルでグレイメールを設定すると、電子メールゲートウェイは IMS のグローバル設定をマシンレベルにコピーします。
- スキャンメッセージの最大メッセージサイズとタイムアウト値が異なる場合、電子メールゲートウェイは最大タイムアウトおよび最大メッセージサイズの値を使用して、IMS とグレイメールのグローバル設定を行います。たとえば、IMS およびグレイメールの最大メッセージサイズの値がそれぞれ 1M と 2M である場合、アプライアンスは IMS とグレイメールの両方の最大メッセージサイズ値として 2M を使用します。

パフォーマンスアドバイザリ

アウトブレイクフィルタ

アウトブレイクフィルタは、コンテキスト適応スキャンエンジンを使用してメッセージの脅威レベルを判定し、アダプティブルールとアウトブレイクルールの組み合わせに基づいてメッセージにスコアを付けます。一部の設定では、中程度のパフォーマンス低下が発生する可能性があります。

IronPort スパム隔離

C シリーズのアプライアンスに対して IronPort スパム隔離オンボックスを有効にすると、公称水準の負荷がかかっているアプライアンスでは、システムスループットにわずかな低下が生じます。ピークスループット付近またはピークスループットで実行されている電子メールゲートウェイの場合、アクティブな隔離からの追加の負荷によって、スループットが 10 ～ 20% 低下する可能性があります。システムのキャパシティがいっぱいか、いっぱいに近いときに IronPort スパム隔離を使用する場合は、規模が大きい C シリーズ アプライアンスまたは M シリーズ アプライアンスへの移行を検討してください。

スパム対策ポリシーをスパムのドロップから隔離に変更する場合（オンボックスまたはオフボックス）、ウイルスおよびコンテンツセキュリティのために追加のスパムメッセージをスキャンする必要があるため、システムの負荷が増大します。インストールのサイジングを適切に行う際にサポートが必要な場合は、認定サポートプロバイダーにお問い合わせください。

既知および修正済みの問題

シスコのバグ検索ツールを使用して、このリリースの既知および修正済みの不具合に関する情報を検索します。

バグ検索ツールの要件

シスコ アカウントを持っていない場合は、登録します。
https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui に移動します。

既知および修正済みの問題のリスト

AsyncOS 15.0.1 の既知および修正済みの問題

既知の問題	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=15.0.1&prdNam=Cisco%20Secure%20Email%20Gateway
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=15.0.1-030&prdNam=Cisco%20Secure%20Email%20Gateway

AsyncOS 15.0 の既知および修正済みの問題

既知の問題	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=15.0.0&prdNam=Cisco%20Secure%20Email%20Gateway
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=15.0.0-104&prdNam=Cisco%20Secure%20Email%20Gateway

既知および解決済みの問題に関する情報の検索

シスコのバグ検索ツールを使用して、既知および解決済みの不具合に関する最新情報を検索します。

はじめる前に

シスコ アカウントを持っていない場合は、登録します。
https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui に移動します。

手順

ステップ 1 https://tools.cisco.com/bugsearch/ に移動します。

ステップ 2 シスコ アカウントのクレデンシャルでログインします。

ステップ 3 [リストから選択(Select from list)] > [セキュリティ(Security)] > [電子メールセキュリティ(Email Security)] > [Cisco Secure Email Gateway] の順にクリックし、[OK] をクリックします。

ステップ 4 [リリース(release)] フィールドに、リリースのバージョン(たとえば、15.0)を入力します

ステップ 5 要件に応じて、次のいずれかを実行します。

- 解決済みの問題のリストを表示するには、[バグの表示(Show Bugs)] ドロップダウンから、[これらのリリースで修正済み(Fixed in these Releases)] を選択します。
- 既知の問題のリストを表示するには、[バグの表示(Show Bugs)] ドロップダウンから [これらのリリースに影響(Affecting these Releases)] を選択し、[ステータス(Status)] ドロップダウンから [開く(Open)] を選択します。

ご不明な点がある場合は、ツールの右上にある [ヘルプ(Help)] または [フィードバック(Feedback)] リンクをクリックしてください。また、インタラクティブなツアーもあります。これを表示するには、[検索(search)] フィールドの上のオレンジ色のバーにあるリンクをクリックします。

関連資料

マニュアルの内容 （Cisco Content Security 製品）	参照先
ハードウェアおよび仮想アプライアンス	この表で該当する製品を参照してください。
Cisco Secure Email and Web Manager	http://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Secure Web Appliance	http://www.cisco.com/c/ja_jp/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco Secure Email ゲートウェイ	http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/tsd-products-support-series-home.html
Cisco Secure Email クラウドゲートウェイ	https://www.cisco.com/c/en/us/support/security/cloud-email-security/products-user-guide-list.html
Cisco Secure Email Gateway CLI リファレンスガイド	http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-command-reference-list.html
Cisco Secure Email Encryption Service	http://www.cisco.com/c/ja_jp/support/security/email-encryption/tsd-products-support-series-home.html

サービスとサポート

（注） 仮想アプライアンスのサポートを受けるには、仮想ライセンス番号（VLN）をご用意の上 Cisco TAC に連絡してください。

Cisco TAC：http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

従来の IronPort のサポートサイト：http://www.cisco.com/web/services/acquisitions/ironport.html

重大ではない問題の場合は、電子メールゲートウェイからカスタマーサポートにアクセスすることもできます。手順については、ユーザーガイドまたはオンラインヘルプを参照してください。